



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/324,308	06/02/1999	STEPHEN MICHAEL MATYAS JR.	5577-159	1364

20792 7590 12/03/2002

MYERS BIGEL SIBLEY & SAJOVEC  
PO BOX 37428  
RALEIGH, NC 27627

EXAMINER

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 12/03/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/324,308	<b>Applicant(s)</b> MATYAS ET AL.	
	<b>Examiner</b> Benjamin E Lanier	<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_\_.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-57 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-5, 9-18, 22-31 and 35-57 is/are rejected.
- 7) ☒ Claim(s) 6-8, 19-21, 32-34 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 02 June 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner. *drafts person*
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56, and 57 are rejected under 35 U.S.C. 102(b) as being anticipated by Pastor, U.S. Patent No. 4,878,246. Referring to claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56, and 57, Pastor discloses a method and apparatus for generating encryption/decryption keys wherein a key is generated from an identification number (user specific information) and where two sets of prime numbers (first and second subinterval) are generated from the identification number. A prime number is then taken from each set (Col. 2, lines 6-42). A memory is used (storage medium) to access the prime numbers and produce the key (Col. 2, lines 19-24).

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 10, 11, 23, 24, 36, 37, 41, 42, 47, 48, 53, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pastor, U.S. Patent No. 4,878,246, in view of Tomko, U.S. Patent No. 5,680,460. Referring to claims 10, 11, 23, 24, 36, 37, 41, 42, 47, 48, 53, and 54,

Pastor discloses a method and apparatus for generating encryption/decryption keys wherein a key is generated from an identification number (user specific information) and where two sets of prime numbers (first and second subinterval) are generated from the identification number. A prime number is then taken from each set (Col. 2, lines 6-42). A memory is used (storage medium) to access the prime numbers and produce the key (Col. 2, lines 19-24). Pastor does not disclose that the user specific information is biometric information. Tomko discloses a user inputting finger print data at the time the user wishes to create a key (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made use biometric data in the method and apparatus for generating keys of Pastor in order to provide an extremely secure private key which is not even known by the user yet is readily accessible as taught in Tomko (Col. 2, lines 17-20).

5. Claims 12, 13, 25, 26, 38, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pastor, U.S. Patent No. 4,878,246, in view of Jablon, U.S. Patent No. 6,226,383. Referring to claims 12, 13, 25, 26, 38, and 39, Pastor discloses a method and apparatus for generating encryption/decryption keys wherein a key is generated from an identification number (user specific information) and where two sets of prime numbers (first and second subinterval) are generated from the identification number. A prime number is then taken from each set (Col. 2, lines 6-42). A memory is used (storage medium) to access the prime numbers and produce the key (Col. 2, lines 19-24). Pastor does not disclose selecting a random point as a starting point for a prime number search. Jablon discloses cryptographic methods where a random point of prime order is chosen. If the starting point is determined to be out of the prescribed range then another value is chosen as the starting point. This starting point is used as

Art Unit: 2132

the basis for the calculation of the prime number to be selected (Col. 15, lines 49-56). It would have been obvious to one of ordinary skill in the art at the time the invention was made to select the prime number of Pastor in the manner of Jablon in order to increase computational efficiency as taught in Jablon (Col. 14, lines 24-29).

6. Claims 43, 49, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pastor, U.S. Patent No. 4,878,246, in view of Dawson, U.S. Patent No. 5,709,114. Referring to claims 43, 49, and 55, , Pastor discloses a method and apparatus for generating encryption/decryption keys wherein a key is generated from an identification number (user specific information) and where two sets of prime numbers (first and second subinterval) are generated from the identification number. A prime number is then taken from each set (Col. 2, lines 6-42). A memory is used (storage medium) to access the prime numbers and produce the key (Col. 2, lines 19-24). Pastor does not disclose using company identification as the entity specific information. Dawson discloses an electronic lock system where a key to the lock contains three elements: personal identifier, company identifier, and authorization level (Col. 4, lines 57-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use company identification information as the entity specific information in Pastor so that a company could generate keys unique to them.

*Allowable Subject Matter*

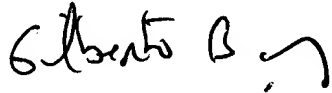
7. Claims 6-8, 19-21, and 32-34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is (703)-305-7684. The examiner can normally be reached on M-Th from 7:30am to 5:00pm, F from 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on (703)-305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703)-746-7239, after final (703)-746-7238, or non-official/draft (703)-746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

  
**GILBERTO BARRON**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**

BL